UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

In re: SAV-RX Data Breach Litigation	Lead Case No. 8:24-cv-00204-RFR-RCC **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR A JURY TRIAL**

Plaintiffs Connor Geerhart, Heather Krueger, Samantha Moser, David Prestby, Derek Summerville, and Tiffany Sutherlin, on behalf of herself and her minor children, K.S, K.S, and K.S. (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint") against Defendant A&A Services, LLC d/b/a Sav-Rx ("Sav-Rx" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to Plaintiffs' own actions and upon information and belief and investigation of their counsel as to all other matters, as follows:

SUMMARY OF ACTION

1. This class action arises from Defendant's failure to implement and maintain adequate data security safeguards, which resulted in a massive data breach that exposed the highly-sensitive personally identifiable information ("PII") and protected health information ("PHI") (together, "Private Information") of Plaintiffs and more than 2.8 million Class Members (the "Data Breach").[1]

2. Sav-Rx is a Nebraska-based pharmacy benefit management company that provides medication benefits management services to thousands of health plan customers and over 10 million individual members of those health plans.[2] To provide those services, Sav-Rx solicits, collects, and stores extensive files of sensitive data belonging millions of individuals, including Plaintiffs and Class Members.

3. The Data Breach was discovered when Sav-Rx detected an interruption to its

[1] U.S. Department of Health & Human Servs. Off. for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information – Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. , 2024).
[2] Sav-Rx, *Home – Benefiting over 10 million American workers and their families*, https://savrx.com/ (last visited Dec. 16, 2024); *see also* Sav-Rx, *Get to know us*, https://savrx.com/story/ (last visited Dec. 16, 2024).

internal computer network on October 8, 2023.[3] Following an investigation, Sav-Rx determined that an unauthorized third party accessed and exfiltrated Private Information from Sav-Rx's systems on October 3, 2023.[4]

4. Individuals affected by the Data Breach include members of Defendant's health plan customers as well as current and former Sav-Rx employees.[5]

5. The Private Information compromised and stolen in the Data Breach includes, without limitation: Plaintiffs' and Class Members' full names, dates of birth, Social Security numbers, email addresses, physical addresses, phone numbers, eligibility data, and insurance identification numbers.[6]

6. Despite learning of the Data Breach on October 8, 2023, Sav-Rx waited more than ***seven months*** to begin notifying individuals affected by the Data Breach.[7]

7. Sav-Rx claims its "initial priority [following discovery of the Data Breach on October 8, 2023] was restoring systems to minimize any interruption to patient care."[8]

8. "After [its] systems were secured," Sav-Rx launched an investigation with the help of third-party cybersecurity experts.[9]

9. According to Sav-Rx, it "received the results of that investigation on April 30, 2024[,]"[10] and the investigation confirmed that the cybercriminals who perpetrated the Data

[3] *A&A Services Frequently Asked Questions*, https://faq.savrx.com / (last visited Dec. 16, 2024).
[4] *Id.*
[5] *Id.*
[6] *Sav-Rx Data Breach Notice Letter*, https://faq.savrx.com/Sav-RX1.0.0_FAQ.pdf (last visited Dec. 16, 2024).
[7] *A&A Services Frequently Asked Questions*, *supra*, https://faq.savrx.com.
[8] *Id.*
[9] *Id.*
[10] *Id.*

Breach accessed and exfiltrated Plaintiffs' and Class Members' Private Information from Sav-Rx's systems.[11]

10. Sav-Rx claims it "confirmed that any data acquired from [its] IT system was destroyed and has not been disseminated any further."[12]

11. Sav-Rx further promised that it has "taken steps to enhance [its] security protocols and controls, technology, policies, and training, and [] will continue to assess further options to protect [its] IT system."[13]

12. Sav-Rx began sending written data breach notices ("Data Breach Notice Letters") to affected individuals, including Plaintiffs and Class Members, on or about May 10, 2024—more than seven months after the Data Breach was discovered.[14]

13. On May 24, 2024—nearly eight months after the Data Breach was discovered—Sav-Rx notified the United States Department of Health and Human Services ("HHS") that at least 2,812,336 individuals were affected by the Data Breach.[15]

14. Plaintiffs and Class Members entrusted their sensitive Private Information to Sav-Rx and/or their respective health insurance plans with the reasonable expectation that their highly-sensitive data would be protected from unauthorized disclosure.

15. By soliciting, collecting, and storing Plaintiffs' and Class Members' Private Information, Sav-Rx assumed statutory, regulatory, contractual, and common law duties and obligations to keep that highly-sensitive data confidential and secure from unauthorized access.

---

[11] *See id.*

[12] *A&A Services Frequently Asked Questions*, *supra*, https://faq.savrx.com.

[13] *Id.*

[14] *See Sav-Rx Data Breach Notice Letter*, *supra*, https://faq.savrx.com/Sav-RX1.0.0_FAQ.pdf.

[15] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, *supra*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

16. In a Notice of Privacy Practices posted on its website, Sav-Rx recognizes that it is "required by law to maintain the privacy and security of [individuals'] protected health information."[16]

17. Sav-Rx also promises patients: "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[17]

18. Despite these assurances, Sav-Rx failed to adequately secure Plaintiffs' and Class Members' highly sensitive Private Information from unauthorized disclosure. Instead, Sav-Rx maintained and shared the Private Information in a negligent and/or reckless manner. Upon information and belief, the Private Information was maintained on computer systems in a condition vulnerable to cyberattacks.

19. Sav-Rx failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information in its custody.

20. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Sav-Rx.

21. The Data Breach was foreseeable because the Private Information solicited, collected, and stored by Sav-Rx is highly valuable due to its unique value to identity thieves.

22. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable data security procedures and protocols to protect the Private Information it solicited, collected, and stored from a foreseeable and preventable cyberattack.

23. As a direct and proximate result of Defendant's failure to implement and maintain

[16] Sav-Rx, *Notice of Privacy Practices* (May 21, 2024), https://savrx.com/privacy-policy-2/ (last visited Dec. 16, 2024).

[17] *Id.*

adequate and reasonable data security measures, Plaintiffs' and Class Members' Private Information is now in the hands of cybercriminals and, upon information and belief, published on the dark web, as evidenced by alerts received by Plaintiffs Moser and Sutherlin.

24. Armed with the Private Information stolen in the Data Breach, data thieves can commit a variety of crimes including, but not limited to: opening new financial accounts and taking out loans in Plaintiffs' and Class Members' names; using Plaintiffs' and Class Members' Private Information to obtain medical services or government benefits; using Plaintiffs' and Class Members' Private Information to target other phishing and hacking intrusions; filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining driver's licenses or other government identification in Plaintiffs' and Class Members' names; and giving false information to police during an arrest.

25. As a result of the Data Breach, at least 2,812,336 Class Members (including Plaintiffs)[18] suffered concrete injuries, including, but not limited to: (a) actual fraud and identity theft; (b) the loss of the opportunity to control how their Private Information is used; (c) the compromise, publication, or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, or unauthorized use of their Private Information; (e) loss of productivity and lost opportunity costs associated with addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (f) costs associated with placing freezes on credit reports; (g) the continued risk and substantially increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

[18] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, *supra*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information; (h) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (i) the diminution in value of Plaintiffs' and Class Members' Private Information; and (j) overpayment for the services that were received without adequate data security.

26. Plaintiffs and Class Members also face a substantial risk of imminent harm as a result of the Data Breach, heightened by the theft of their Social Security numbers, a type of Private Information which is particularly valuable to identity thieves.

27. This risk is even more pronounced given the unreasonable and extended time between when Sav-Rx discovered the Data Breach and when Sav-Rx notified Plaintiffs and Class Members that their Private Information had been improperly accessed and stolen by cybercriminals.

28. Plaintiffs and Class Members have suffered—and will continue to suffer—injuries associated with this risk, including but not limited to loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

29. Plaintiffs and Class Members have already incurred—and will continue to incur—out-of-pocket costs for, *inter alia*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

30. Sav-Rx disregarded and violated the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs

and Class Members prompt and accurate notice of the Data Breach.

31. Accordingly, Plaintiffs bring this action against Sav-Rx, seeking redress for Sav-Rx's unlawful conduct and asserting claims for: (i) negligence; (ii) negligence *per se*; (iii) breach of bailment; (iv) invasion of privacy/intrusion upon seclusion; (v) breach of implied contract; (vi) breach of third-party beneficiary contract; (vii) unjust enrichment; (viii) breach of fiduciary duty; and (ix) declaratory judgment. Through these claims, Plaintiffs seek damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Sav-Rx's data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by Sav-Rx.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs, and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant, there are more than 100 putative Class Members, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

33. This Court has jurisdiction over Defendant because Defendant operates in and directs commerce to this District and Defendant's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District, rendering the exercise of jurisdiction by this Court just and proper.

34. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

PARTIES

35. Defendant A&A Services, LLC d/b/a Sav-Rx is a limited liability company organized under the state laws of Nebraska with its principal place of business in Fremont, Nebraska.

Plaintiff Connor Geerhart

36. Plaintiff Connor Geerhart is a natural person and citizen of the state of Washington. He resides in Spokane, Washington, where he intends to remain.

37. Plaintiff Geerhart is a current participant of a health plan serviced by Defendant.

38. As a condition of obtaining medication benefit management services from Defendant, Plaintiff Geerhart was required to provide his PII and PHI to Defendant, including his name, address, date of birth, Social Security number, phone number, email address, and insurance identification number.

39. At the time of the Data Breach, Defendant maintained Plaintiff Geerhart's PII and PHI in its system.

40. Defendant obtained and continues to maintain Plaintiff Geerhart's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

41. Plaintiff Geerhart is very careful about sharing his sensitive personal information. Plaintiff Geerhart takes proactive steps to ensure his PII and PHI are kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Geerhart would not have entrusted his PII and PHI to Defendant had he known of Defendant's lax data security practices.

42. Plaintiff Geerhart received the Notice Letter, by U.S. mail, directly from Defendant, dated May 19, 2024 – over seven months after the breach occurred. According to the Notice Letter,

Plaintiff Geerhart's PII and PHI were improperly accessed and obtained by unauthorized third parties, including his name, address, date of birth, and Social Security number.

43. As a result of the Data Breach, Plaintiff Geerhart took reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit reports and statements, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Geerhart has spent significant time dealing with the Data Breach—valuable time Plaintiff Geerhart otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

44. Plaintiff Geerhart suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) lost or diminished value of his PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

45. Plaintiff Geerhart additionally suffered actual injury in the form of increased phishing emails and targeted advertising regarding his medical condition for which he receives prescription medication from Sav-Rx. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Geerhart's life, and specifically caused stress and strain on him as

a direct result of the Data Breach.

46. The Data Breach has also caused Plaintiff Geerhart to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

47. As a result of the Data Breach, Plaintiff Geerhart anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

48. As a result of the Data Breach, Plaintiff Geerhart is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

49. Plaintiff Geerhart has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

Plaintiff Heather Krueger

50. Plaintiff Heather Krueger is a natural person and citizen of the state of Wisconsin. She resides in Watertown, Wisconsin, where she intends to remain.

51. Plaintiff Krueger is a current/former participant of a health plan serviced by Defendant.

52. As a condition of obtaining medication benefit management services from Defendant, Plaintiff Krueger was required to provide her PII and PHI to Defendant, including her name, address, date of birth, Social Security number, phone number, email address, and insurance identification number.

53. At the time of the Data Breach, Defendant maintained Plaintiff Krueger's PII and PHI in its system.

54. Defendant obtained and continues to maintain Plaintiff Krueger's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

55. Plaintiff Krueger is very careful about sharing her sensitive personal information. Plaintiff Krueger takes proactive steps to ensure her PII and PHI are kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Krueger would not have entrusted her PII and PHI to Defendant had she known of Defendant's lax data security practices.

56. Plaintiff Krueger received the Notice Letter, by U.S. mail, directly from Defendant, dated May 19, 2024 – over seven months after the breach occurred. According to the Notice Letter, Plaintiff Krueger's PII and PHI were improperly accessed and obtained by unauthorized third parties, including her name, address, date of birth, and Social Security number.

57. As a result of the Data Breach, Plaintiff Krueger made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Krueger has spent significant time dealing with the Data Breach—valuable time Plaintiff Krueger otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

58. Plaintiff Krueger suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII and PHI, which: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

59. Plaintiff Krueger additionally suffered actual injury in the form of increased spam emails and texts, and targeted advertisements. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Krueger's life, and specifically caused anxiety and strain on her as a direct result of the Data Breach.

60. The Data Breach has also caused Plaintiff Krueger to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

61. As a result of the Data Breach, Plaintiff Krueger anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

62. As a result of the Data Breach, Plaintiff Krueger is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

63. Plaintiff Krueger has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

Plaintiff Samantha Moser, on behalf of herself and her minor children, D.P., Z.M., C.M., and W.M.

64. Plaintiff Samantha Moser and her minor children, D.P., Z.M., C.M., and W.M, are natural persons and citizens of the Commonwealth of Pennsylvania. Plaintiff Moser resides in Bristol, Pennsylvania, where she intends to remain.

65. Plaintiff Moser is a current participant of a health plan serviced by Defendant. Plaintiff's four minor children—D.P., Z.M., C.M., and W.M—are also covered under her health plan.

66. As a condition of obtaining medication benefit management services from Defendant, Plaintiff Moser and her minor children were required to provide their PII and PHI to Defendant, including their names, addresses, dates of birth, Social Security numbers, phone numbers, email addresses, and insurance identification numbers.

67. At the time of the Data Breach, Defendant maintained Plaintiff Moser's and her minor children's PII and PHI in its system.

68. Defendant obtained and continues to maintain Plaintiff Moser's and her minor children's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

69. Plaintiff Moser is very careful about sharing her and her children's sensitive personal information. Plaintiff Moser takes proactive steps to ensure that her and her children's PII and PHI are kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Moser would not have entrusted her or her children's PII or PHI to Defendant had she known of Defendant's lax data security practices.

70. Plaintiff Moser received the Notice Letter, by U.S. mail, directly from Defendant, dated May 19, 2024 – over seven months after the breach occurred. According to the Notice Letter,

Plaintiff Moser's PII and PHI were improperly accessed and obtained by unauthorized third parties, including her name, address, date of birth, and Social Security number.

71. Plaintiff Moser also received four additional Notice Letters directly from Defendant, by U.S. mail, addressed to Plaintiffs' four minor children, and each is dated May 19, 2024. According to these Notice Letters, the PII and PHI of each of Plaintiff's minor children was improperly accessed and obtained by unauthorized third parties, including their names, addresses, dates of birth, and Social Security numbers.

72. As a result of the Data Breach, Plaintiff Moser made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Moser has spent significant time dealing with the Data Breach—valuable time Plaintiff Moser otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

73. Plaintiff Moser suffered actual injury from having her and her children's PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of their PII and PHI; (iii) lost or diminished value of their PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII and PHI, which: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

74. Shortly after the Data Breach, Plaintiff Moser suffered additional actual injury in the form of fraudulent access to her Venmo account, which was associated with the same email address that she provided to Sav-Rx.

75. Following the Data Breach, Plaintiff Moser also received alerts from her bank that her PII and PHI—including her name, address, date of birth, Social Security number, and email address—have been detected on the dark web. Plaintiff Moser began receiving those alerts in November 2023, shortly after the Sav-Rx Data Breach.

76. Plaintiff Moser has also experienced a noticeable uptick in spam and phishing texts, emails, and phone calls following the Data Breach.

77. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Moser's life, and specifically caused anxiety and strain on her as a direct result of the Data Breach. Plaintiff Moser is particularly concerned by the exposure of her minor children's PII and PHI.

78. The Data Breach has also caused Plaintiff Moser and her minor children to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from their PII and PHI being placed in the hands of criminals.

79. As a result of the Data Breach, Plaintiff Moser anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

80. As a result of the Data Breach, Plaintiff Moser and her minor children are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

81. Plaintiff Moser has a continuing interest in ensuring that her and her minor children's PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

Plaintiff David Prestby

82. Plaintiff David Prestby is a natural person and citizen of the state of Minnesota. He resides in Brownsville, Minnesota, where he intends to remain.

83. Upon information and belief, Plaintiff Prestby is a current participant of a health plan serviced by Defendant.

84. As a condition of obtaining medication benefit management services from Defendant, Plaintiff Prestby was required to provide his PII and PHI to Defendant, including his name, address, date of birth, Social Security number, phone number, email address, and insurance identification number.

85. At the time of the Data Breach, Defendant maintained Plaintiff Prestby's PII and PHI in its system.

86. Defendant obtained and continues to maintain Plaintiff Prestby's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

87. Plaintiff Prestby is very careful about sharing his sensitive personal information. Plaintiff Prestby takes proactive steps to ensure his PII and PHI are kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Prestby would not have entrusted his PII and PHI to Defendant had he known of Defendant's lax data security practices.

88. Plaintiff Prestby received the Notice Letter, by U.S. mail, directly from Defendant, dated May 18, 2024 – over seven months after the breach occurred. According to the Notice Letter, Plaintiff Prestby's PII and PHI were improperly accessed and obtained by unauthorized third parties, including his name, address, date of birth, Social Security number, and phone number.

89. As a result of the Data Breach, Plaintiff Prestby made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, signing up for credit monitoring and identity theft protection services through Equifax as offered by Defendant, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Prestby has spent significant time dealing with the Data Breach—valuable time Plaintiff Prestby otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

90. Plaintiff Prestby suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) lost or diminished value of his PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

91. Plaintiff Prestby additionally suffered actual injury in the form of lost time Plaintiff

Prestby spent resetting all his account passwords. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Prestby's life, and specifically caused fear, anxiety, and strain on him as a direct result of the Data Breach.

92. The Data Breach has also caused Plaintiff Prestby to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

93. As a result of the Data Breach, Plaintiff Prestby anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

94. As a result of the Data Breach, Plaintiff Prestby is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

95. Plaintiff Prestby has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

Plaintiff Derek Summerville

96. Plaintiff Derek Summerville is a natural person and citizen of the state of Ohio. He resides in Akron, Ohio where he intends to remain.

97. Plaintiff Summerville is a current participant of a health plan serviced by Defendant.

98. As a condition of obtaining medication benefit management services from Defendant, Plaintiff Summerville was required to provide his PII and PHI to Defendant, including his name, address, date of birth, Social Security number, phone number, email address, and insurance identification number.

99. At the time of the Data Breach, Defendant maintained Plaintiff Summerville's PII and PHI in its system.

100. Defendant obtained and continues to maintain Plaintiff Summerville's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

101. Plaintiff Summerville is very careful about sharing his sensitive personal information. Plaintiff Summerville takes proactive steps to ensure his PII and PHI are kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Summerville would not have entrusted his PII and PHI to Defendant had he known of Defendant's lax data security practices.

102. Plaintiff Summerville received the Notice Letter, by U.S. mail, directly from Defendant, dated May 19, 2024 – over seven months after the breach occurred. According to the Notice Letter, Plaintiff Summerville's PII and PHI were improperly accessed and obtained by unauthorized third parties, including his name, address, date of birth, and Social Security number.

103. As a result of the Data Breach, Plaintiff Summerville made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Summerville has spent significant time dealing with the Data Breach—valuable time Plaintiff Summerville otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

104. Plaintiff Summerville suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy;

(ii) theft of his PII and PHI; (iii) lost or diminished value of his PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

105. Plaintiff Summerville additionally suffered actual injury in the form of receiving frequent spam calls. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Summerville's life, and specifically caused stress and strain on him as a direct result of the Data Breach, as he no longer answers phone calls.

106. The Data Breach has also caused Plaintiff Summerville to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

107. As a result of the Data Breach, Plaintiff Summerville anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

108. As a result of the Data Breach, Plaintiff Summerville is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

109. Plaintiff Summerville has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

Plaintiff Tiffany Sutherlin, on behalf of herself and her minor children K.S., K.S., and K.S.

110. Plaintiff Tiffany Sutherlin and her minor children, K.S., K.S., and K.S. are natural persons and citizens of the state of Missouri. She resides in Saint Louis, where she intends to remain. Plaintiff Tiffany Sutherlin is a former participant of a health plan serviced by Defendant.

111. In addition, Plaintiff's three minor children, K.S., K.S., and K.S. were covered under Plaintiff's health plan serviced by Defendant.

112. As a condition of obtaining medication benefit management services from Defendant, Plaintiff Sutherlin and her minor children were required to provide their PII and PHI to Defendant, including their names, addresses, dates of birth, Social Security numbers, email address, phone numbers, and insurance identification numbers.

113. At the time of the Data Breach, Defendant maintained Plaintiff Sutherlin's and her children's PII and PHI in its system.

114. Defendant obtained and continues to maintain Plaintiff Sutherlin's and her children's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

115. Plaintiff Sutherlin is very careful about sharing her and her children's sensitive personal information. Plaintiff Sutherlin takes proactive steps to ensure her and her children's PII and PHI are kept safe and secure and would never knowingly transmit unencrypted sensitive information over the internet. Thus, Plaintiff Sutherlin would not have entrusted her and her children's PII and PHI to Defendant had she known of Defendant's lax data security practices.

116. Plaintiff Sutherlin received the Notice Letter, by U.S. mail, directly from Defendant, dated May 19, 2024 – over seven months after the breach occurred. According to the Notice Letter, Plaintiff Sutherlin's PII and PHI were improperly accessed and obtained by

unauthorized third parties, including her name, address, date of birth, Social Security number, phone number, and insurance identification number.

117. Plaintiff Sutherlin received three additional Notice Letters directly from Defendant, by U.S. mail, each of which is addressed to each of Plaintiff's three minor children, and each is dated May 19, 2024. According to these Notice Letters, the PII and PHI of each of Plaintiff's minor children was improperly accessed and obtained by unauthorized third parties, including their names, addresses, dates of birth, Social Security numbers, and insurance identification numbers.

118. As a result of the Data Breach, Plaintiff Sutherlin was notified by Credit Karma—a personal finance company—that her PII and PHI were detected on the dark web.

119. As a result of the Data Breach, Plaintiff Sutherlin made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, driving to her financial institutions to secure her accounts and resolve any fraudulent transactions, and speaking on the phone with her credit card companies to verify and combat any fraudulent credit card transactions. The fraudulent activity on her financial and credit card accounts may take years to detect. Plaintiff Sutherlin has spent significant time dealing with the Data Breach—valuable time Plaintiff Sutherlin otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

120. Plaintiff Sutherlin suffered actual injury from having her and her children's PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of her PII and PHI; (iv) lost time and money spent out-of-pocket associated with attempting to mitigate the actual consequences of the Data Breach, including spending over $50.00 in gasoline to be able to drive to her financial institutions to secure her accounts from fraud and paying for monthly credit

monitoring; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including losing out on a contract accounting project worth over $1,000.00 in labor; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII and PHI, which: (a) remain unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

121. Plaintiff Sutherlin additionally suffered actual injury in the form of receiving increased spam calls, social media direct messages, emails, and text messages, and having her compromised PII and PHI leaked on the dark web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Sutherlin's life, and specifically caused fear, anxiety, stress, and strain on her because—as a direct result of the Data Breach—not only are her PII and PHI exposed, but so are the PII and PHI of her children. Since Plaintiff's children have their whole lives ahead of them, Plaintiff is concerned of others taking advantage of her children's exposed PII and PHI.

122. The Data Breach has also caused Plaintiff Sutherlin and her children to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from their PII and PHI being placed in the hands of criminals.

123. As a result of the Data Breach, Plaintiff Sutherlin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused to her and her children by the Data Breach.

124. As a result of the Data Breach, Plaintiff Sutherlin and her children are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Sutherlin and her children have a continuing interest in ensuring that their PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, are protected and safeguarded from future breaches.

FACTUAL ALLEGATIONS

Defendant's Business

125. Sav-Rx provides medication benefits management services to its health plan customers and millions of individual members of those health plans.[19]

126. Sav-Rx boasts that its "pioneering services enable nearly 1,000 Union Health and Welfare Funds, other plan sponsors, and millions of American workers and their families who rely upon them for benefits to maintain affordable access to life-changing medications, maximizing their well-being at the lowest net cost."[20]

127. To provide those services, Sav-Rx solicits, collects, and stores extensive files of sensitive data belonging to millions of individuals, including Plaintiffs and Class Members.

128. According to Sav-Rx, in the course of "provid[ing] medication benefit management services to health plans, [] [Sav-Rx] receive[s] certain information from health plans and health care providers to deliver these services."[21]

129. Upon information and belief, in the ordinary course of its business, Sav-Rx solicits, collects, stores, and maintains the Private Information of consumers, including but not limited to:

---

[19] *Home – Benefiting over 10 million American workers and their families*, *supra*, https://savrx.com/; *see also Get to know us*, *supra*, https://savrx.com/story/.

[20] Sav-Rx, *Flip the script in YOUR benefit*, https://savrx.com/flip-the-script/ (last visited Dec. 16, 2024).

[21] *See Sav-Rx Data Breach Notice Letter*, *supra*, https://faq.savrx.com/Sav-RX1.0.0_FAQ.pdf.

- Names, addresses, phone numbers and email addresses;
- Dates of birth;
- Demographic information;
- Social Security numbers or taxpayer identification numbers;
- Financial and/or payment information;
- Health billing information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health information; and
- Other information that Sav-Rx may deem necessary to provide services and care.

130. Additionally, Sav-Rx may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, other doctors, health plans, close friends, and/or family members.

131. Plaintiffs and Class Members are current and former members of health plans serviced by Sav-Rx, and current and former employees of Sav-Rx.

132. Plaintiffs and Class Members were required to provide their Private Information to Sav-Rx (and/or their health plan providers) as a condition of receiving medical services from Sav-Rx.

133. By soliciting, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Sav-Rx assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

134. Because of the highly sensitive and personal nature of the information Sav-Rx acquires and stores with respect to consumers and other individuals, Sav-Rx, upon information and belief, promises to, among other things: keep Private Information private; comply with industry standards related to data security and Private Information, including HIPAA and FTC guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiffs and Class Members obtain from Sav-Rx and provide adequate notice to individuals if their Private Information is disclosed without authorization.

135. Sav-Rx also promised to provide confidentiality and adequate security for Plaintiffs' and Class Members' Private Information through its applicable privacy policy and through other disclosures made in compliance with statutory privacy requirements.[22]

136. In a Notice of Privacy Practices posted on its website, Sav-Rx recognizes that it is "required by law to maintain the privacy and security of [individuals'] protected health information[,]"[23] and promises to "let [individuals] know promptly if a breach occurs that may have compromised the privacy or security of [their] information."[24]

137. Contrary to those promises, however, Sav-Rx failed to implement and maintain adequate data security to protect its systems from unauthorized access, and it waited more than seven months to publicly disclose the Data Breach to affected individuals.

138. Plaintiffs and Class Members relied on Sav-Rx's promises to keep their sensitive Private Information confidential and securely maintained, to use that information for business purposes only, and to make only authorized disclosures of that information.

---

[22] *See Notice of Privacy Practices*, *supra*, https://savrx.com/privacy-policy-2/.
[23] *Id.*
[24] *Id.*

The Data Breach and Notice Letter

139. Sav-Rx discovered the Data Breach on October 8, 2023, when it detected an interruption to its internal computer network.[25]

140. A subsequent investigation confirmed that an unauthorized third party improperly accessed Sav-Rx's internal systems and exfiltrated Plaintiffs' and Class Members' Private Information on October 3, 2023.[26]

141. More than seven months later—on or about May 10, 2024—Sav-Rx began sending Data Breach Notice Letters to Plaintiffs and Class Members, informing them:

> **WHAT HAPPENED?**
>
> On October 8, 2023, we identified an interruption to our computer network. As a result, we immediately took steps to secure our systems and engaged third-party cybersecurity experts. Our information technology systems ("IT System") were restored the next business day, and prescriptions were shipped on time without delay.
>
> As part of the investigation, we learned that an unauthorized third party was able to access certain non-clinical systems and obtained files that contained health information. After an extensive review with third-party experts, on April 30, 2024, we discovered that some of the data accessed or acquired by the unauthorized third party may have contained your protected health information. Based on the results of the forensic investigation, we believe the unauthorized third party first accessed the IT System on or around October 3, 2023.
>
> **WHAT INFORMATION WAS INVOLVED?**
>
> The information that may have been accessed or acquired included your name, address, date of birth, and social security number.[27]

[25] *A&A Services Frequently Asked Questions*, *supra*, https://faq.savrx.com/.

[26] *Id.*

[27] *Sav-Rx Data Breach Notice Letter*, *supra*, https://faq.savrx.com/Sav-RX1.0.0_FAQ.pdf.

142. The Data Breach Notice Letters fail to provide critical facts about the Data Breach. Critical information omitted from the Data Breach Notice Letters includes: the identity of the cybercriminals who perpetrated the Data Breach, details about the root cause of the Data Breach, the mechanism of the Data Breach, and the vulnerabilities exploited by the threat actors. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected. Without this information, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

143. According to the Data Breach Notice Letters, Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

144. Sav-Rx claims that it "worked in conjunction with outside cybersecurity experts to contain the incident and confirm any data acquired from our IT System was destroyed and not further disseminated."[28]

145. Upon information and belief, the data stolen in the Data Breach contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

146. Due to Sav-Rx's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

147. Following the Data Breach, Sav-Rx promised that it "took a number of detailed and immediate mitigation measures," including: "24/7 security operations center, Microsoft Defender anti-virus and firewall, multi-factor authentication, BitLocker, Zabbix, new firewall and switches,

[28] *Id*.

patching cycle implementation, network segmentation, Linux system hardening, enhanced geo-blocking, LAPS installation, SSL certification cycling, website/portal enhancements, and policy and procedure development. We continue to analyze additional opportunities for enhancing our security posture."[29]

148. Sav-Rx had obligations created by the FTC Act, HIPAA, contract, common law, industry standards, and its own affirmative representations to keep Plaintiffs' and Class Members' Private Information confidential and secure from unauthorized access and disclosure.

149. But Sav-Rx failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the sensitive information it solicited, collected, stored, and maintained.

The Data Breach Was a Foreseeable Risk of Which Defendant Was on Notice

150. At all relevant times, Sav-Rx knew, or should have known, that Plaintiffs' and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Sav-Rx failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that they should have anticipated and guarded against.

151. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches targeting healthcare entities that collect and store Private Information.

152. Cybercriminals target institutions which collect and store PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were at least 905 health data breaches in 2021, impacting over 50 million

[29] *A&A Services Frequently Asked Questions*, *supra*, https://faq.savrx.com/.

patients. The report noted that "the volume and impact of breaches continue to be underreported overall, and underrepresented to the public[,]" stressing that "gaps in detection and reporting mean the true impact of incidents is likely even greater."[30]

153. Cyberattacks against the healthcare industry have become so frequent that the FBI and U.S. Secret Service have issued warnings to potential targets to be prepared for a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[31]

154. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[32]

155. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only

[30] Protenus, Inc. & DataBreaches.net, *2022 Breach Barometer®: Hackers Exploit Healthcare Industry's Insider Risks, Resource Limitations*, https://www.protenus.com/hubfs/Breach_Barometer/BreachBarometer_Privacy_2022_Protenus.pdf?utm_campaign=Forbes%2520Articles&utm_source=forbes&utm_medium=article&utm_content=breach%2520barometer (last visited Dec. 16, 2024).

[31] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019) https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Dec. 16, 2024).

[32] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited Dec. 16, 2024).

> threaten the privacy and security of patients' health and financial information, but also patient access to care.[33]

156. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into medical practices for their highly prized medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights (OCR)] – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[34]

157. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[35] In this case, Sav-Rx stored Private Information belonging to *millions* of patients.

158. Healthcare partner and provider companies, like Sav-Rx, have been frequent targets of recent data breaches, including: HCA Healthcare (11 million plan members, July 2023), Managed Care of North America (8 million plan members, March 2023), PharMerica Corporation (5 million plan members, March 2023), HealthEC LLC (4 million plan members, July 2023), ESO Solutions, Inc. (2.7 million plan members, September 2023), Prospect Medical Holdings, Inc. (1.3 million plan members, July-August 2023).

---

[33] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Dec. 16, 2024).

[34] Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, The HIPAA Journal (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records (last visited Dec. 16, 2024).

[35] *See id.*

159. In light of these recent high profile cybersecurity incidents at other healthcare partner and provider companies, at all relevant times, Sav-Rx knew or should have known that its electronic records and patients' Private Information were likely to be targeted by cybercriminals.

160. At all relevant times, Sav-Rx knew, or reasonably should have known, the importance of safeguarding Plaintiffs' and Class Members' Private Information and the foreseeable consequences that would occur if their systems were breached, including the significant costs that Plaintiffs and Class Members would incur as a result of a breach.

161. Sav-Rx also knew or should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

The Data Breach Was Preventable

162. According to the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[36]

163. To prevent and detect cyber-attacks and/or ransomware attacks, Sav-Rx could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[36] U.S. Dep't of Justice, *How to Protect Your Networks from RANSOMWARE*, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 20, 2024).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[37]

[37] *Id.* at 3-4.

164. To prevent and detect cyber-attacks or ransomware attacks, Sav-Rx could and should have implemented, the following measures:

- **Secure Internet-Facing Assets**
    - Apply latest security updates
    - Use threat and vulnerability management
    - Perform regular audit; remove privileged credentials;
- **Thoroughly investigate and remediate alerts**
    - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
    - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
    - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
- **Apply principle of least-privilege**
    - Monitor for adversarial activities
    - Hunt for brute force attempts
    - Monitor for cleanup of Event Logs
    - Analyze logon events;
- **Harden infrastructure**
    - Use Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[38]

[38] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster* (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Dec. 16, 2024).

165. Sav-Rx could and should have implemented all of the above measures to prevent and detect cyberattacks.

166. The occurrence of the Data Breach indicates that Sav-Rx failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than 2.8 million individuals, including Plaintiffs and Class Members.

Defendant Failed to Comply With FTC Guidelines

167. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices, including the need for data security to be factored into all business decision-making.

168. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[39]

169. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[40]

---

[39] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 16, 2024).

[40] *Id.*

170. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

171. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

172. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

173. Sav-Rx failed to properly implement basic and reasonably available data security practices.

174. Sav-Rx's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

175. Sav-Rx was at all times fully aware of its obligation to protect the Private Information it collected and stored. Sav-Rx was also aware of the significant repercussions that

would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

176. As noted above, experts studying cybersecurity routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

177. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Sav-Rx, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data. Sav-Rx failed to follow these industry best practices, including a failure to implement multi-factor authentication.

178. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. Sav-Rx failed to follow these cybersecurity best practices, including failure to train staff.

179. Upon information and belief, Sav-Rx failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls

(CIS CSC), which are all established standards in reasonable cybersecurity readiness.

180. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Sav-Rx failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Failed to Comply with HIPAA Guidelines

181. Sav-Rx is a covered entity under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

182. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

183. Sav-Rx is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

184. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

185. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

186. Title II of HIPAA contains what are known as the Administrative Simplification

provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306 (a)(1-4); 45 C.F.R. § 164.312 (a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308 (a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

187. A data breach such as the one Sav-Rx experienced, is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

188. The Data Breach resulted from a combination of insufficiencies that demonstrate Sav-Rx failed to comply with safeguards mandated by HIPAA regulations.

Data Breaches Put Consumers at Substantially Increased Risk of Fraud

189. Cyberattacks and data breaches at healthcare service providers like Sav-Rx are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

190. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[41]

191. A study by Experian found that the "average total cost" of medical identity theft

[41] *See* U.S. Gov't Accountability Off., *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 16, 2024).

was "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[42]

192. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal Private Information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities to engage in illegal financial transactions under the victims' names.

193. Private Information remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[43]

194. Private Information can be sold at a price ranging from $40 to $200.[44] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[45]

195. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[46] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10

---

[42] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Dec. 16, 2024).

[43] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec. 16, 2024).

[44] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 16, 2024).

[45] VPNOverview, *In the Dark* (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec. 16, 2024).

[46] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Dec. 16, 2024) (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating, "Health information is a treasure trove for criminals").

personal identifying characteristics of an individual."[47]

196. Moreover, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

197. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

198. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [48] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[49]

199. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and Class Members, can lead to identity theft and extensive financial fraud:

---

[47] *Id.*

[48] *See* Soc. Security Admin. Philadelphia Region, *Avoid Identity Theft: Protect Social Security Numbers,* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited Dec. 16, 2024).

[49] *Id.*

> Scammers use your Social Security number (SSN) to get other personal information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.[50]

200. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[51] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[52]

201. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[53] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

202. Moreover, it is no easy task to change or cancel a stolen Social Security number.

203. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be

---

[50] Soc. Security Admin., *Identity Theft and Your Social Security Number* (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 16, 2024).

[51] Equifax, *How to Protect Yourself from Social Security Number Identity Theft*, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited Dec. 16, 2024).

[52] Julia Kagan, *What is an SSN? What to Know About Social Security Numbers*, Investopedia (Sept. 2, 2024), https://www.investopedia.com/terms/s/ssn.asp (last visited Dec. 16, 2024).

[53] *Id.*

effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[54]

204. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

205. Similarly, the California state government warns plan members that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit

[54] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Dec. 16, 2024).

and bank accounts, rent an apartment, or even get a job."[55]

206. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names. "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[56]

207. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

208. Private Information, like that stolen from Sav-Rx, is "often processed and packaged with other illegally obtained data to create full record sets ("Fullz" packages)[57] that contain

---

[55] *See* State of California Dept. of Justice, *Your Social Security Number: Controlling the Key to Identity Theft*, https://oag.ca.gov/idtheft/facts/your-ssn (last visited Dec. 16, 2024).

[56] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 16, 2024).

[57] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning

extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[58]

209. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

210. There may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

211. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

GAO Report at 29.

---

credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited Dec. 16, 2024).

[58] *See id.*

212. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

213. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' Private Information secure are severe and long-lasting.

214. To avoid detection, identity thieves often hold stolen data for months or years before using it.

215. The sale of stolen information on the "dark web" can also take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Cybercriminals are known to sell data piecemeal to maximize the value of a hack, extending the duration of the risk to victims for years following the date of a breach.

216. Plaintiffs and Class Members must therefore vigilantly monitor their financial and medical accounts for many years to come.

217. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[59]

Plaintiffs' and Class Members' Damages

218. Given the sensitivity of the Private Information involved in the Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of

[59] *See* Fed. Trade Comm'n, *What To Do Right Away: What To Do Next*, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Dec. 16, 2024).

additional injuries for years to come, if not the rest of their lives.

219. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

220. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

221. Upon information and belief, Plaintiffs' and Class Members' Private Information has already been published for sale on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

222. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time and resources dealing with the effects of the Data Breach.

223. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

224. Plaintiffs and Class Members also face a substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

225. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

226. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have

recognized the propriety of loss of value damages in similar cases.

227. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Sav-Rx and/or Sav-Rx's healthcare partners was intended to be used by Sav-Rx to fund adequate security of their computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

228. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

229. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance

accounts, bank accounts, and credit reports for unauthorized activity for years to come.

230. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Sav-Rx, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

231. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

232. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs propose the following Class definition, subject to amendment as appropriate:

Nationwide Class

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendant in May 2024, including all persons who received notice of the Data Breach (the "Class" or "Nationwide Class").

Washington Subclass

All individuals residing in Washington whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendant in May 2024, including all persons who received notice of the Data Breach (the "Washington Subclass").

Pennsylvania Subclass

All individuals residing in Pennsylvania whose Private Information was accessed and/or acquired by an unauthorized party as a result of

the Data Breach reported by Defendant in May 2024, including all persons who received notice of the Data Breach (the "Pennsylvania Subclass").

Ohio Subclass

All individuals residing in Ohio whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendant in May 2024, including all persons who received notice of the Data Breach (the "Ohio Subclass").

Missouri Subclass

All individuals residing in Missouri whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendant in May 2024, including all persons who received notice of the Data Breach (the "Missouri Subclass").

233. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family plan members.

234. Plaintiffs reserve the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

235. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 2,812,336 individuals were affected by the Data Breach.[60]

[60] U.S. Dep't of Health and Human Servs. Off. for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information – Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 16, 2024).

236. Commonality: There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

237. Typicality: Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

238. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

239. Predominance: Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the data of Plaintiffs and Class Members was stored on the same network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

240. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum

simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

241. The nature of this action and the laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

242. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

243. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

244. Unless a Class-wide injunction is issued, Defendant may continue in its failure to

properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

245. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

246. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient PII and PHI; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

247. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

COUNT I
Negligence

(On Behalf of Plaintiffs and the Nationwide Class)

248. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

249. Defendant owes a duty under common law to Plaintiffs and Class Members to exercise reasonable care in safeguarding, securing, and protecting the highly sensitive and confidential patient data it solicits, collects, stores, and maintains.

250. Defendant owes a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, and other requirements discussed herein, to ensure that its systems and networks, and the personnel responsible for them, adequately secure and protect the Private Information that Defendant solicits, collects, stores, and maintains.

251. Defendant's duty to use reasonable data security measures includes, among other things: (a) designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and Class Members is adequately secured and protected; (b) removing or deleting sensitive patient data when no longer needed for authorized purposes; (c) implementing and maintaining procedures to detect and prevent improper access to and misuse of Plaintiffs' and Class Members' Private Information.

252. Defendant's duty to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' Private Information arises from several sources,

including, but not limited to, those described below.

253. By soliciting, accepting, storing, and maintaining Plaintiffs' and Class Members' Private Information, Defendant undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

254. Defendant solicits, collects, stores, and maintains the Private Information of Plaintiffs and Class Members as part of its regular business practice.

255. Defendant required Plaintiffs and Class Members to entrust it with their Private Information to receive healthcare services.

256. Defendant's business model depends on its ability to solicit, collect, store, and maintain troves of highly sensitive information that patients – including Plaintiffs and Class Members – are required to provide to receive healthcare services.

257. Defendant exercised control over the Private Information stored on its systems and networks; accordingly, they were best positioned and most capable of preventing the harms caused by the Data Breach.

258. Plaintiffs and Class Members were not in a position to assess the data security practices Defendant purportedly used.

259. Because Plaintiffs and Class Members had no means to identify or assess Defendant's data security deficiencies, Plaintiffs and Class Members had no opportunity to safeguard their Private Information from cybercriminals.

260. Defendant therefore knew or reasonably should have known that Plaintiffs and Class Members relied on them to secure and protect their highly sensitive Private Information from unauthorized access and disclosure.

261. Plaintiffs and Class Members entrusted Sav-Rx with their Private Information in order to receive healthcare services and with the mutual understanding and reasonable expectation that Sav-Rx would safeguard their highly sensitive and confidential data.

262. Defendant's duty to use reasonable data security measures to protect and secure Plaintiffs' and Class Members' Private Information therefore arises from the special relationship that exists between Defendant and Plaintiffs and Class Members.

263. Defendant's failure to implement and maintain adequate data security created a foreseeable risk that Plaintiffs' and Class Members' Private Information would be improperly accessed or disclosed to unauthorized third parties in a data breach.

264. Defendant has, and at all relevant times had, full knowledge of the sensitivity of Plaintiffs' and Class Members' Private Information and the type of harm Plaintiffs and Class Members could and would suffer if their Private Information was compromised or wrongfully disclosed to unauthorized third parties in a data breach.

265. Defendant knew or reasonably should have known that their failure to exercise due care in soliciting, collecting, storing, and using Plaintiffs' and Class Members' Private Information would expose Plaintiffs and Class Members to a foreseeable risk of unreasonable harm.

266. Defendant had long known, or had reason to know, that its electronic record-keeping systems were prime targets for hackers.

267. Past breaches in the healthcare industry put Defendant on notice that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, and Defendant knew or should have known that the risk of a data breach was highly likely. Indeed, upon information and belief, Defendant belongs to or receives alerts from H-ISAC, the Health Information Sharing and Analysis Center, "a global, non-profit, member-driven

organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating, and sharing vital physical and cyber threat intelligence and best practices with each other."

268. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's failure to implement and maintain adequate data security practices and procedures.

269. Despite being aware of the risk of cyberattacks and the inadequacy of their own systems, Defendant failed to implement and maintain adequate data security practices, resulting in the compromise and exposure of Plaintiffs' and Class Members' Private Information in the Data Breach.

270. Defendant failed to heed industry warnings and alerts to implement adequate data security safeguards to protect Plaintiffs' and Class Members' Private Information.

271. That Plaintiffs and Class Members would be harmed, and the types of harm actually experienced by Plaintiffs following the Data Breach, were foreseeable consequences of Defendant's failure to implement adequate data security practices.

272. Defendant has admitted that Plaintiffs' and Class Members' Private Information was accessed and exfiltrated by unauthorized third parties in the Data Breach.

273. Defendant had and continues to have a duty to adequately disclose if and when Private Information stored on its systems or networks is compromised, including how the data was compromised, the precise types of data that were compromised, and when. Such notice was and remains necessary to enable Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft or fraudulent misuse of their Private Information by third parties.

274. Defendant breached its duties to Plaintiffs and Class Members by failing to use reasonable measures to protect their Private Information. The specific negligent acts and omissions

committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate and industry-standard data security protocols to protect and safeguard Plaintiffs' and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to detect and prevent unauthorized access to Plaintiffs' and Class Members' Private Information;

d. Failing to remove or delete Private Information it was no longer required to retain pursuant to regulations; and

e. Failing to timely and adequately notify Plaintiffs and Class Members about the occurrence and scope of the Data Breach.

275. Defendant's failure to implement adequate data security measures and oversight procedures to protect Plaintiffs' and Class Members' Private Information caused Plaintiffs and Class Members to suffer injuries when their Private Information was accessed and stolen by unauthorized third parties in the Data Breach.

276. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' Private Information would not have been compromised in the Data Breach.

277. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach as a direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding that information by adopting, implementing, and maintaining appropriate data security measures.

278. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class

Members have suffered and will suffer injuries, including, but not limited to: (a) actual fraud and identity theft; (b) the loss of the opportunity to control how their Private Information is used; (c) the compromise, publication, or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, or unauthorized use of their Private Information; (e) loss of productivity and lost opportunity costs associated with addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (f) costs associated with placing freezes on credit reports; (g) the continued risk and substantially increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information; (h) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (i) the diminution in value of Plaintiffs' and Class Members' Private Information; and (j) overpayment for the services that were received without adequate data security.

279. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury or harm, including, but not limited to, loss of privacy and other economic and non-economic losses.

280. Plaintiffs and Class Members have a present and continuing interest in the security of their Private Information, which upon information and belief remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its custody.

281. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT II
Negligence *Per Se*

(On behalf of Plaintiffs and the Nationwide Class)

282. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

283. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information as part of its regular business, which affects commerce.

284. Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, and the various state consumer protection statutes discussed herein are independent sources of Defendant's duty to use reasonable data security measures to protect Plaintiffs' and Class Members' Private Information.

285. The relevant requirements imposed by Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, and state statutory law inform Defendant's duty of care.

286. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to employ reasonable measures to protect and secure sensitive consumer data. The FTC publications and orders described herein also form part of the basis of Defendant's duty in this regard.

287. Defendant also has a duty to use reasonable data security measures under HIPAA, which requires covered entities and their business associates, like Defendant, to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure." 45 C.F.R. Part 164. HIPAA also specifically requires "administrative, physical, and technical safeguards to secure

[] PII and PHI." *Id.*

288. Defendant's violations of Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, and state statutory law constitute negligence *per se*.

289. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTC Act, the HIPAA Privacy and Security Rules, and state consumer protection statutes were intended to protect.

290. The FTC has long recognized that Section 5 of the FTC Act applies to "unfair" or "deceptive" acts that "cause[] substantial injury to consumers[,]" and numerous courts have held that Section 5 of the FTC Act was designed to protect consumers whose data was compromised by the negligent acts of a defendant. 29 Fed. Reg. 8324, 8355 (July 2, 1964).

291. HIPAA was enacted to establish a set of standards and requirements for the transmission of certain health information. 45 C.F.R. §160.103(3). Plaintiffs and Class Members are patients seeking to vindicate their right to privacy in their Private Information, and to be protected from Defendant's inadequate data security practices—interests at the very core of HIPAA.

292. The harm Plaintiffs and Class Members suffered as a result of Defendant's failure to implement and maintain adequate data security is the type of harm that Section 5 of the FTC Act and the HIPAA Privacy and Security Rules were intended to guard against.

293. The FTC has pursued enforcement actions against businesses, like Defendant, which, as a result of their failure to employ reasonable data security measures, caused the same types of harm suffered by Plaintiffs and the Class as a result of the Data Breach.

294. Defendant breached its duty to secure and safeguard Plaintiffs' and Class Members' Private Information by violating statutory laws requiring them to implement and maintain adequate

data security to safeguard consumers' personal information.

295. Defendant's duty to use reasonable care in protecting Plaintiffs' and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect and secure Private Information in its possession and control.

296. It was reasonably foreseeable to Defendant that its failure to implement and maintain adequate data security practices to safeguard and protect Plaintiffs' and Class Members' Private Information would result in the improper access and disclosure of that sensitive information to unauthorized third parties.

297. Defendant's conduct was particularly unreasonable given the nature and amount of patient Private Information it solicits, collects, stores, and maintains, and the foreseeable consequences of a data breach, including the substantial damages that would result to Plaintiffs and the Class in the event of a data breach.

298. The injury and harm Plaintiffs and Class Members suffered following the Data Breach were the direct and proximate result of Defendant's violations of Section 5 of the FTC Act and the HIPAA Privacy and Security Rules.

299. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injuries, including, but not limited to: (a) actual fraud and identity theft; (b) the loss of the opportunity to control how their Private Information is used; (c) the compromise, publication, or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, or unauthorized use of their Private Information; (e) loss of productivity and lost opportunity costs associated with addressing and attempting to mitigate the present and continuing consequences of the Data Breach,

including but not limited to efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (f) costs associated with placing freezes on credit reports; (g) the continued risk and substantially increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information; (h) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (i) the diminution in value of Plaintiffs' and Class Members' Private Information; and (j) overpayment for the services that were received without adequate data security.

300. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

301. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risk of exposure of their Private Information, which upon information and belief remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

302. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
Breach of Bailment

(On behalf of Plaintiffs and the Nationwide Class)

303. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

304. Plaintiffs' and Class Members' Private Information is personal property and was conveyed to Defendant for the certain purpose of keeping that information private and confidential.

305. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendant was aware of the risks it took when soliciting, collecting, and storing Plaintiffs' and Class Members' Private Information, and it assumed the risk voluntarily.

306. Once Defendant accepted Plaintiffs' and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within Defendant's possession, custody, and control.

307. Plaintiffs and Class Members provided their Private Information to Defendant with the mutual understanding and reasonable expectation that Defendant would implement and maintain adequate data security to protect Plaintiffs' and Class Members' confidential data from unauthorized access and disclosure.

308. Defendant did not safeguard Plaintiffs' and Class Members' Private Information when it failed to implement and maintain adequate data security safeguards to protect against the known risk of a cyberattack.

309. Defendant's failure to secure and safeguard Plaintiffs' and Class Members' Private Information resulted in that information being accessed and obtained by unauthorized third parties.

310. As a direct and proximate result of Defendant's failure to keep Plaintiffs' and Class Members' Private Information secure, Plaintiffs and Class Members suffered injuries, as alleged

herein, for which compensation—including actual, consequential, and nominal damages—is appropriate.

COUNT IV
Invasion of Privacy/Intrusion Upon Seclusion

(On behalf of Plaintiffs and the Nationwide Class)

311. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

312. Plaintiffs and Class Members have a legitimate expectation of privacy in their Private Information, and they are entitled to the protection of that information against improper access and disclosure to unauthorized third parties.

313. As alleged, Defendant owes a duty to Plaintiffs and Class Members to keep their Private Information secure and confidential.

314. Defendant failed, however, to implement and maintain adequate data security practices to secure and protect Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure.

315. By failing to adequately protect Plaintiffs' and Class Members' Private Information, Defendant allowed unauthorized and unknown third parties to access and obtain Plaintiffs' and Class Members' private and confidential data.

316. The unauthorized access and disclosure of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

317. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

318. Plaintiffs and Class Members entrusted their Private Information to Defendant in

order to receive Defendant's services, but they did so privately, with the intention, mutual understanding, and reasonable expectation that their Private Information would be kept confidential and protected from unauthorized access and disclosure.

319. Plaintiffs and Class Members reasonably expected that the Private Information they entrusted to Defendant would be kept private and would not be disclosed without their authorization.

320. Defendant's inadequate data security practices, polices, and procedures, including vendor management, and the resulting Data Breach, constitute intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

321. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it knew or should have known that its data security practices were inadequate.

322. Past breaches in the healthcare industry put Defendant on clear notice that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information, and Defendant knew or should have known that the risk of a data breach was highly likely.

323. Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's failure to implement and maintain adequate data security practices and procedures.

324. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that

would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

325. Defendants knew or reasonably should have known that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

326. As a direct and proximate result of the above acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to third parties without their authorization, causing Plaintiffs and Class Members to suffer damages.

327. Defendant's unlawful invasions of privacy damaged Plaintiffs and Class Members, as alleged herein. Among other things, Plaintiffs and Class Members have suffered mental distress, and their reasonable expectations of privacy have been frustrated and defeated.

328. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial and/or injunctive relief.

COUNT V
Breach of Implied Contract

(On behalf of Plaintiffs and the Nationwide Class)

329. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

330. When Plaintiffs and Class Members entrusted Defendant with their Private Information, they did so with the reasonable expectation that Defendant would protect their highly sensitive and confidential data from unauthorized access and disclosure.

331. Plaintiffs and Class Members were required to provide their Private Information to Defendant in exchange for receiving healthcare services.

332. Defendant offered healthcare services to Plaintiffs in exchange for payment, and Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of that transaction.

333. Defendant solicited and accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing healthcare services to Plaintiffs and Class Members.

334. In connection with receiving those healthcare services, Plaintiffs and Class Members entered into implied contracts with Defendant.

335. Pursuant to the implied contracts, Plaintiffs and Class Members paid money to Defendant for the provision of healthcare services, directly or through their insurance, and entrusted Defendant with their Private Information.

336. In exchange for Plaintiffs' and Class Members' payments for healthcare services, Defendant implicitly agreed to secure and protect the Private Information it required Plaintiffs and Class Members to provide.

337. Plaintiffs, Class Members, and Defendant had a mutual understanding that Defendant would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiffs' and Class Members' Private Information. Plaintiffs, Class Members, and Defendant also shared an expectation and understanding that Defendant would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in their possession and control.

338. Pursuant to the implied contracts, Defendant agreed to, and Plaintiffs and Class Members mutually understood and reasonably expected that Defendant would, among other things: (a) provide healthcare services to Plaintiffs and Class Members; (b) take reasonable and legally and contractually required measures to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information; (c) take reasonable and legally and contractually required steps to ensure that access to the Private Information in the possession and control of Defendant was restricted and limited to achieve an authorized medical purpose; (d) restrict access to qualified and trained agents and vendors; (e) design and implement appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (f) require proper encryption of the Private Information; (g) require multifactor authentication for access to the Private Information; and (h) otherwise protect Plaintiffs' and Class Members' Private Information in compliance with federal and state laws, regulations, and industry standards.

339. The protection of Plaintiffs' and Class Members' Private Information was a material term of the implied contracts between Plaintiffs and Class Members and Defendant.

340. Indeed, Defendant knew data security was an important factor in Plaintiffs' and Class Members' decision to entrust it with their Private Information.

341. Defendant's public statements proclaiming its commitment to data security, and the promises contained in its privacy policy, indicate Defendant understood its obligation to secure and safeguard Plaintiffs' and Class Members' Private Information.

342. In turn, Plaintiffs and Class Members never would have entrusted Defendant with their Private Information without an implicit assurance that the information would be protected.

343. Had Plaintiffs and Class Members known that Defendant would not adequately protect their Private Information, they would not have sought healthcare services from Defendant, nor would they have entrusted their Private Information to Defendant.

344. Plaintiffs and Class Members fully performed their obligations under the implied contracts when they provided Defendant with their Private Information and paid for healthcare services.

345. The healthcare services rendered by Defendant to Plaintiffs and Class Members, which required Plaintiffs and Class Members to entrust Defendant with their Private Information, were rendered in such a manner as to reflect the mutual understanding that Defendant would adequately secure and protect Plaintiffs' and Class Members' Private Information.

346. When Defendant required Plaintiffs and Class Members to entrust it with their Private Information to receive healthcare services, they manifested by their conduct their mutual understanding of an implied contract to safeguard that Private Information.

347. Defendant breached its obligations under the implied contracts with Plaintiffs and Class Members by failing to implement and maintain reasonable data security measures to protect and secure Plaintiffs' and Class Members' Private Information.

348. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including foreseeable and consequential damages that Defendant knew about when they solicited and collected Plaintiffs' and Class Members' Private Information.

349. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT VI
Breach Of Third-Party Beneficiary Contract

(On Behalf of Plaintiffs and the Nationwide Class)

350. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

351. According to Defendant's Notice of Privacy Practices: "When Sav-Rx provides pharmacy benefit administration services for your health plan, the terms of the contract between your health plan and Sav-Rx governs our handling of your health information."[61]

352. Defendant entered into written contracts, including, upon information and belief, HIPAA Business Associate Agreements, to provide medication benefits management services to Plaintiffs' and Class Members' respective health insurance plans.

353. Those contracts were made expressly for the benefit of Plaintiffs and Class Members, whose confidential medical information Defendant solicited, collected, stored, and maintained, to provide medical benefits management services to Plaintiffs' and Class Members' respective health insurance plans.

354. Plaintiffs and Class Members were the intended beneficiaries of the contracts entered into by Defendant and Plaintiffs' and Class Members' respective health insurance plans – there would be no need for Defendant's medical benefits management services aside from the benefit to Plaintiffs and Class Members. The contracts between Defendant and Plaintiffs' and Class Members' respective health insurance plans were therefore clearly intended for the benefit of Plaintiffs and Class Members, and the benefits of those contracts were directed at Plaintiffs and Class Members.

355. That Plaintiffs and Class Members would rely on the contracts between Defendant

[61] Sav-Rx, *Notice of Privacy Practices*, *supra*, https://savrx.com/privacy-policy-2/.

and their respective health insurance plans to ensure the security of their Private Information was foreseeable to Defendant.

356. Defendant breached its contracts with Plaintiffs' and Class Members' respective health insurance plans when it failed to use reasonable data security measures to adequately protect Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure.

357. Plaintiffs and Class Members were foreseeably harmed by Defendant's failure to use reasonable data security measures, as alleged herein.

358. Accordingly, Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT VII
Unjust Enrichment

(On Behalf of Plaintiffs and the Nationwide Class)

359. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

360. Defendant knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on data security at the expense and to the detriment of Plaintiffs and Class Members.

361. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of monies paid to Defendant for healthcare services.

362. Plaintiffs and Class Members also conferred a benefit upon Defendant through the provision of their Private Information, which has monetary value and from which Defendant derives its business.

363. Defendant solicited, collected, stored, and maintained Plaintiffs' and Class Members' Private Information, and as such, Defendant accepted and had knowledge of the benefits

conferred upon it by Plaintiffs and Class Members. Defendant profited from these transactions and used Plaintiffs' and Class Members' Private Information for business purposes.

364. There is a direct nexus between the money paid to Defendant and the requirement that Defendant keep Plaintiffs' and Class Members' Private Information confidential and protected from unauthorized access and disclosure.

365. Data security was an integral part of the healthcare services Plaintiffs and Class Members paid for.

366. When Plaintiffs and Class Members conferred monetary payments and provided their Private Information to Defendant, they did so with the mutual understanding and reasonable expectation that Defendant would adequately secure and protect their sensitive data from unauthorized access and disclosure.

367. A portion of the payments made by or on behalf of Plaintiffs and Class Members was therefore to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

368. Upon information and belief, Defendant funds its data security measures entirely from its general revenue.

369. Protecting Plaintiffs' and Class Members' Private Information is integral to the Defendant's business. Without Plaintiffs' and Class Members' private data, Defendant would be unable to provide the healthcare services comprising its core business.

370. Instead of providing a reasonable level of data security that would have prevented the Data Breach, however, Defendant calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures.

371. Defendant cut data security costs and failed to take known and available steps to secure and safeguard Plaintiffs' and Class Members' Private Information.

372. Defendant therefore enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

373. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decisions to prioritize its own profits over the requisite data security.

374. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data security measures.

375. Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to adequately provide the data security that Plaintiffs and Class Members paid for and was otherwise mandated by federal, state, and local laws and industry standards.

376. Plaintiffs and Class Members have no adequate remedy at law.

377. It would be inequitable and unconscionable to permit Defendant to retain funds it saved by shirking data security and leaving Plaintiffs and Class Members to suffer the consequences.

378. Defendant should therefore be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains they unjustly received.

COUNT VIII
Breach of Fiduciary Duty / Breach of Confidence

(On behalf of Plaintiffs and the Nationwide Class)

379. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

380. Plaintiffs and Class Members provided their highly sensitive Private Information to Defendant in confidence, with the mutual understanding and reasonable expectation that Defendant would safeguard and protect that information from improper access and disclosure to unauthorized third parties.

381. Plaintiffs and Class Members were required to entrust their Private Information to Defendant to receive and pay for healthcare services, but Plaintiffs and Class Members would not have provided Defendant with their Private Information had they known that their data would not be adequately protected.

382. Defendant's solicitation, acceptance, and storage of Plaintiffs' and Class Members' Private Information, in exchange for healthcare services, created a fiduciary relationship between Defendant on the one hand, and Plaintiffs and Class Members, on the other hand.

383. As a result, Defendant owe Plaintiffs and Class Members fiduciary duties to keep Plaintiffs' and Class Members' Private Information confidential, based on the duty of good faith and the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

384. In light of this relationship, Defendant has a duty to act primarily for the benefit of its patients, which includes a duty to safeguard and protect the Private Information that Plaintiffs and Class Members entrusted to it in order to receive healthcare services.

385. Due to the nature of the relationship between Defendant and Plaintiffs and Class Members, Plaintiffs and Class Members were entirely reliant on Defendant to ensure their Private Information was adequately protected.

386. Plaintiffs and Class Members were not in a position to assess, verify, or influence the data security practices employed by Defendant.

387. Defendant exercised control over the Private Information stored on its systems and networks; accordingly, it was best positioned and most capable of preventing the harms caused by the Data Breach.

388. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement and maintain adequate data security measures to secure and safeguard Plaintiffs' and Class Members' Private Information.

389. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injuries, including, but not limited to: (a) actual fraud and identity theft; (b) the loss of the opportunity to control how their Private Information is used; (c) the compromise, publication, or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, or unauthorized use of their Private Information; (e) loss of productivity and lost opportunity costs associated with addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (f) costs associated with placing freezes on credit reports; (g) the continued risk and substantially increased risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information; (h) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; (i) the diminution in value of Plaintiffs' and Class Members' Private Information; and (j) overpayment for the services that were received without adequate data security.

390. Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury or harm, including, but not limited to, loss of privacy and other economic and non-economic losses.

391. Additionally, as a direct and proximate result of Defendant's breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will suffer the continued risk of exposure of their Private Information, which upon information and belief remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

392. Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT IX
Violation of the Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602

(On Behalf of Plaintiffs and the Nationwide Class)

393. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

394. Plaintiffs and Class Members are "persons" under the Nebraska Consumer Protection Act.

395. Defendant conducts business in Nebraska and/or owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska.

396. Defendant was required to implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, including safeguards that protect the personal information when the individual or

commercial entity disposes of the personal information. Neb. Rev. Stat. § 87-808.

397. Defendant failed to implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information.

398. "A violation of section 87-808 shall be considered a violation of section 59-1602 and be subject to the Consumer Protection Act and any other law which provides for the implementation and enforcement of section 59-1602." Neb. Rev. Stat. § 87-806(2).

399. Defendant's failure to implement and maintain reasonable security protocols to protect the security of millions of individuals' Private Information injures the public interest.

400. Plaintiffs and the Class are entitled to damages under Nebraska Revised Statute § 59-1609.

COUNT X
Violation of Washington Consumer Protection Act
RCW 19.86.010, *et seq.*

(On behalf of Plaintiff Geerhart and the Washington Subclass)

401. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

402. The Washington State Consumer Protection Act, RCW 19.86.020 (the "WCPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the WCPA and relevant case law.

403. Defendant is a "person" as described in RCW 19.86.010(1).

404. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2)

in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

405. By virtue of the wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, as described herein, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the WCPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

406. Defendant's failure to safeguard the PII and PHI exposed in the Data Breach constitutes an unfair act that offends public policy.

407. Defendant's failure to safeguard the PII and PHI compromised in the Data Breach caused substantial injury to Plaintiff Geerhart and Washington Subclass Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

408. Defendant's failure to safeguard the PII and PHI disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

409. In the course of conducting its business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff Geerhart's and Washington Subclass Members' Private Information and violating the common law alleged herein in the process. Plaintiff Geerhart and Washington Subclass Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts

or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

410. Defendant also violated the WCPA by failing to timely notify, and by concealing from Plaintiff Geerhart and Washington Subclass Members, information regarding the unauthorized release and disclosure of their PII and PHI. If Plaintiff Geerhart and Washington Subclass Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information.

411. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the WCPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

412. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

413. Defendant's unfair or deceptive acts or practices occurred in their trade or business and have injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

414. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the WCPA, Plaintiff Geerhart and Washington Subclass Members

have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII and PHI; (5) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

415. Unless restrained and enjoined, Defendant will continue to engage in the wrongful conduct (detailed *supra*) and more data breaches will occur. Plaintiff Geerhart, therefore, on behalf of himself and the Washington Subclass, seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII and PHI entrusted to it.

416. Plaintiff Geerhart, on behalf of himself and Washington Subclass Members, also seeks to recover actual damages sustained by each Washington Subclass Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiff Geerhart, on behalf of himself and Washington Subclass Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Washington Subclass Member by three times the actual damages sustained not to exceed $25,000.00 per Washington Subclass Member.

COUNT XI
Violation of Washington Data Breach Disclosure Law
RCW 19.255.005, *et seq.*

(On behalf of Plaintiff Geerhart and the Washington Subclass)

417. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

418. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

419. Upon information and belief, this statute applies to Defendant because Defendant does not own nor license the PII and PHI in question. Instead, the owners and/or licensees of the PII and PHI are Plaintiffs and the Class.

420. The Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

421. Defendant failed to disclose that the Private Information—of Plaintiffs and Class Members—that had been compromised "immediately" upon discovery, and instead waited more than seven months after discovering the Data Breach to begin notifying Plaintiffs and Class Members. Defendant therefore unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach.

422. Thus, Defendant violated the Washington Data Breach Disclosure Law.

COUNT XII
Violation of Washington Uniform Health Care Information Act (UHCIA)
RCW 70.02.005, *et seq.*

(On behalf of Plaintiff Geerhart and the Washington Subclass)

423. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

424. The Washington Uniform Health Care Information Act ("UHCIA") provides that:

a. "Health care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests." § 70.02.005(1).

b. "In order to retain the full trust and confidence of patients, health care providers have an interest in assuring that health care information is not improperly disclosed and in having clear and certain rules for the disclosure of health care information." § 70.02.005(3).

c. "It is the public policy of this state that a patient's interest in the proper use and disclosure of the patient's health care information survives even when the information is held by persons other than health care providers." § 70.02.005(4).

425. Upon information and belief, Defendant is a "health care provider" within the meaning of the UHCIA because it is "licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." § 70.02.010(19).

426. Under § 70.02.020, "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written

authorization."

427. Defendant violated the UHCIA because Defendant—via the Data Breach—disclosed health care information to third parties without patient authorization.

428. Accordingly, Plaintiffs seek, *inter alia*, all civil remedies available under § 70.02.170, including actual damages, attorneys' fees, and reasonable expenses.

COUNT XIII
Violation of Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 P.S. §§ 201-1-201-9.3

(On Behalf of Plaintiff Samantha Moser and the Pennsylvania Subclass)

429. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

430. Defendant sells and performs services in the Commonwealth of Pennsylvania.

431. Plaintiff Moser, Pennsylvania Subclass Members, and Defendant are "persons" as defined by the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). 73 P.S. § 201-2(2).

432. Defendant's products and services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

433. Defendant obtained Plaintiff Moser's and Pennsylvania Subclass Members' Private Information in connection with the services it performs and provides.

434. Defendant engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable data security measures to protect and secure consumers' (such as Plaintiff Moser's and Pennsylvania Subclass Members') Private Information in a manner that complied with applicable laws, regulations, and industry standards, including by failing to control all environments into which it placed consumers' Private Information, and to

ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

435. As alleged above, Sav-Rx makes explicit statements and promises to its customers that their Private Information will remain private and secure.

436. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). Defendant's failure to adequately protect Plaintiff Moser's and Pennsylvania Subclass Members' Private Information while representing that it would adequately protect that Private Information falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

437. Due to the Data Breach, Plaintiff Moser and Pennsylvania Subclass Members have lost property in the form of their Private Information. Further, Defendant's failure to adopt reasonable practices in protecting and safeguarding patients' Private Information will force

Plaintiff Moser and Pennsylvania Subclass Members to spend time and/or money to protect against identity theft. Plaintiff Moser and Pennsylvania Subclass Members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendant's practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

438. As a result of Defendant's violations of the UTPCPL, Plaintiff Moser and Pennsylvania Subclass Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft, justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

439. Pursuant to 73 P.S. § 201-9.2(a), Plaintiff Moser and Pennsylvania Subclass Members seek actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiff Moser also seeks costs and reasonable attorneys' fees.

COUNT XIV
Violation of the Ohio Consumer Sales Practices Act
ORC §§ 1345, *et seq.*

(On Behalf of Plaintiff Derek Summerville and the Ohio Subclass)

440. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247

as if fully set forth herein.

441. Plaintiff Summerville and Ohio Subclass Members are "consumers" as defined by ORC § 1345.01(D). 299.

442. Sav-Rx advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

443. Sav-Rx engaged in unfair and deceptive acts and practices in the conduct of a consumer transaction, in violation of ORC § 1345.02 and unconscionable consumer sales acts and practices in violation of ORC § 1345.03, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Summerville's and Ohio Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Summerville's and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with Ohio's Data Security Act, ORC § 1354, which provides an affirmative defense to any cause of action in tort brought under Ohio law for failure to implement reasonable information security controls resulting in a data breach involving personal or restricted information. ORC § 1354.02(D)(2);

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff

Summerville's and Ohio Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Summerville's and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Summerville's and Ohio Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Summerville's and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

444. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Sav-Rx's data security and ability to protect the confidentiality of consumers' Private Information.

445. Had Sav-Rx disclosed to Plaintiff Summerville and Ohio Subclass Members that its data systems were not secure and thus vulnerable to attack, Sav-Rx would have been forced to adopt reasonable data security measures and comply with the law. Sav-Rx was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff Summerville and the Ohio Subclass. Sav-Rx accepted the responsibility of protecting the data, while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Summerville and the Ohio Subclass Members acted reasonably in relying on Defendant's

misrepresentations and omissions, the truth of which they could not have discovered.

446. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and practices, Plaintiff Summerville and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including, but not limited to, one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of Private Information; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; lost benefits of bargains as well as overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

447. Plaintiff Summerville and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under ORC § 1345.09(A); declaratory and injunctive relief under ORC § 1345.09(D); reasonable attorneys' fees and costs, under ORC § 1345.09(F); and any other relief that is just and proper.

COUNT XV
Violation of Missouri Merchandising Practices Act
Mo. Rev. Stat. § 407.010, *et seq.*

(On Behalf of Plaintiff Tiffany Sutherlin and the Missouri Subclass)

448. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

449. Mo. Rev. Stat. §407.020 prohibits the use of any "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce[.]"

450. An "unfair practice" is defined by Missouri law, 15 CSR 60-8.020, as any practice which either:

a. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the FTC, or its interpretive decisions; or

b. Is unethical, oppressive or unscrupulous; and presents a risk of, or causes, substantial injury to consumers.

451. Moreover, 15 CSR 60-8.040 provides that an unfair practice is: "An unfair practice for any person in connection with the advertisement or sale of merchandise to violate the duty of good faith in solicitation, negotiation and performance, or in any manner fail to act in good faith[.]"

452. Plaintiff Tiffany Sutherlin and Missouri Subclass Members are "persons" within the meaning of Mo. Rev. Stat. § 407.010(5).

453. Merchandise is defined by the Missouri Merchandising Practices Act ("MMPA"), to include the providing of "services" and, therefore, encompasses healthcare services. Healthcare services are a "good" within the meaning of the statute.

454. Efforts to maintain the privacy and confidentiality of medical records are part of the healthcare services associated with a good.

455. Maintenance of medical records are "merchandise" within the meaning of section Mo. Rev. Stat. § 407.010(4).

456. The goods and/or services Plaintiff Sutherlin and Missouri Subclass Members purchased and/or received from Sav-Rx were for "personal, family or household purposes" within the meaning of the MMPA.

457. As set forth herein, Defendant's acts, practices, and conduct violate Mo. Rev. Stat. § 407.010(1) in that, among other things, Sav-Rx has used and/or continues to use unfair practices, concealment, suppression, and/or omission of material facts in connection with the advertising, marketing, and offering for sale of services associated with healthcare services. Such acts offend the public policy established by Missouri statute and constitute an "unfair practice" as that term is used in Mo. Rev. Stat. § 407.020(1).

458. Defendant's unfair, unlawful, and deceptive acts, practices and conduct include: (a) representing to patients—including Plaintiff Sutherlin and Missouri Subclass Members—that it will not disclose their sensitive Private Information to any unauthorized third party or parties; (b) failing to implement security measures such as securing the records in a safe place; (c) failing to train personnel; and (d) charging patients for privacy services which were not provided.

459. Sav-Rx's conduct also violates the enabling regulations for the MMPA because it: (a) offends public policy; (b) is unethical, oppressive and unscrupulous; (c) causes substantial injury to consumers; (d) it is not in good faith; (e) is unconscionable; and (f) is unlawful. Mo. Code Regs. Ann tit. 15, Section 60-8.

460. As a direct result of Defendant's breach of its duty of confidentiality and privacy

and the disclosure of Plaintiff Sutherlin's and the Missouri Subclass Members' Private Information, Plaintiff Sutherlin and Missouri Subclass Members suffered damages, including: (a) loss of the benefit of the bargain; (b) exposure to heightened future risk of identity theft; (c) loss of privacy, confidentiality; and (d) anxiety, embarrassment, humiliation, and loss of enjoyment of life.

461. As a direct and proximate result of Sav-Rx's unfair and deceptive acts, Plaintiff Sutherlin and the Missouri Subclass Members suffered damages in that they paid for data security and privacy protections they did not receive. In this respect, Plaintiff Sutherlin and Missouri Subclass Members did not receive the benefit of their bargains and have suffered ascertainable loss.

462. Plaintiff Sutherlin and Missouri Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

COUNT XVI
Declaratory Judgment (28 U.S.C. § 2201)

(On behalf of Plaintiffs and the Nationwide Class)

1. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 247 as if fully set forth herein.

2. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. §2201.

3. As previously alleged, Defendant owed a duty of care to Plaintiffs and the Class that requires it to adequately secure and protect Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure.

4. Upon information and belief, Defendant still possesses Plaintiffs' and Class Members' Private Information.

5. Defendant failed to fulfill its contractual and legal duties to secure and safeguard Plaintiffs' and Class Members' Private Information.

6. As described herein, Plaintiffs have suffered actual harm in the wake of the Data Breach. Plaintiffs and the Class are also at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the data security failings that led to such exposure.

7. Plaintiffs and the Class, therefore, seek a declaration that: (a) Defendant's existing data security and vendor management measures do not comply with its contractual obligations and duties of care to adequately secure Plaintiffs' and Class Members' Private Information; and (b) to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable data security measures, including, but not limited to:

a. Engaging internal security personnel to conduct testing, including audits of Defendant's systems on a periodic basis, and promptly correcting any problems or issues detected by such internal security auditors;

b. Engaging third-party security auditors to run automated security monitoring of Defendant's computer networks;

c. Auditing, testing, and training its security personnel and employees regarding any new or modified data security policies and procedures;

d. Purging, deleting, and destroying, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. Conducting regular database scanning and security checks;

f. Implementing mechanisms, procedures, and vendor management policies to adequately oversee the data security of any companies Defendant contracts with and with which it entrusts highly sensitive personal information, including but not limited to, Plaintiffs' and Class Members' Private Information; and

g. Routinely and continually conducting internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Plaintiffs' and Class Members' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, request judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: December 16, 2024

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates
Markovits, Stock & DeMarco, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
T: (513) 651-3700
F: (513) 665-0219
E: tcoates@msdlegal.com

Charles E. Schaffer
Levin Sedran & Berman LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
T: (215) 592-4663
E: cschaffer@lfsblaw.com

Kate M. Baxter-Kauf
Lockridge Grindal Nauen PLLP
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
T: (612) 339-6900
E: kmbaxter-kauf@locklaw.com

James J. Pizzirusso
Hausfeld LLP
888 16th Street, NW, Suite 300
Washington, DC 20006
T: (202) 540-7200
E: jpizzirusso@hausfeld.com

Jean S. Martin
Morgan & Morgan Complex Litigation Group
201 North Franklin Street, 7th Floor
Tampa, FL 33606
T: (813) 223-5505
E: jeanmartin@forthepeople.com

Courtney E. Maccarone
Levi & Korsinsky, LLP
33 Whitehall Street, 17 Floor
New York, NY 10004
T: (212) 363-7500
E: cmaccarone@zlk.com

Interim Co-Lead Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that I served the foregoing upon all parties through their counsel of record by filing it with the Court's electronic-filing system in accordance with Fed. R. Civ. P. 5(b)(2)(E).

/s/ Terence R. Coates
Terence R. Coates